UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

LIONRA TECHNOLOGIES LIMITED,

Plaintiff,

v.

CISCO SYSTEMS, INC.,

Defendant.

Case No. 2:22-cv-305

JURY TRIAL DEMANDED

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Lionra Technologies Limited ("Lionra") files this complaint against Cisco Systems, Inc. ("Cisco" or "Defendant"), alleging infringement of U.S. Patent Nos. 7,916,630, 8,566,612, 7,921,323, 7,302,708, and 7,685,436 ("Patents-in-Suit"). The Accused Products are computer networking and security products made, used, offered for sale, sold, imported by Defendant in the United States and supplied by Defendant to its customers and integrated into electronic devices sold in the United States.

Plaintiff Lionra and the Patents-in-Suit

1. Plaintiff Lionra is a technology licensing company organized under the laws of Ireland, with its headquarters at The Hyde Building, Suite 23, The Park, Carrickmines, Dublin 18, Ireland.

2. Lionra is the owner of U.S. Patent No. 7,916,630, entitled "Monitoring Condition of Network with Distributed Components," which issued March 29, 2011 (the "'630 patent"). A copy of the '630 patent is attached to this complaint as Exhibit 1.

3. Lionra is the owner of U.S. Patent No. 8,566,612, entitled "System and Method for a Secure I/O Interface," which issued October 2, 2013 (the "'612 patent"). A copy of the '612 patent is attached to this complaint as Exhibit 2.

4. Lionra is the owner of U.S. Patent No. 7,921,323, entitled "Reconfigurable Communications Infrastructure for ASIC Networks," which issued November 16, 2006 (the "'323 patent"). A copy of the '323 patent is attached to this complaint as Exhibit 3.

5. Lionra is the owner of U.S. Patent No. 7,302,708, entitled "Enforcing Computer Security Utilizing an Adaptive Lattice Mechanism," which issued November 27, 2007 (the "'708 patent"). A copy of the '708 patent is attached to this complaint as Exhibit 4.

6. Lionra is the owner of U.S. Patent No. 7,685,436, entitled "System and Method for a Secure I/O Interface," which issued March 23, 2010 (the "'436 patent"). A copy of the '436 patent is attached to this complaint as Exhibit 5.

Defendant and the Accused Products

7. On information and belief, Defendant Cisco is a California corporation with its principal place of business at 170 West Tasman Drive, San Jose, California 95134. Cisco can be served through its registered agent, Prentice Hall Corporation System, 211 E. 7th Street, Suite 620, Austin, TX 78701.

8. The Accused Products include firewall products such as the Cisco Firepower 4100 and the Cisco Secure Web Application Firewall, aggregation router products such as the Cisco ASR 901, wireless access points such as the Cisco Catalyst 9100, network switch products such as the Cisco Catalyst 9500.

Jurisdiction and Venue

9. This action arises under the patent laws of the United States, Title 35 of the United States Code. This Court has original subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

10. This Court has personal jurisdiction over Cisco in this action because, among other reasons, Cisco has committed acts within the Eastern District of Texas giving rise to this action and has established minimum contacts with the forum state of Texas. Cisco maintains several places of business within the State, including at 2250 East President George Bush Turnpike, Richardson, TX 75082. Cisco directly and/or through subsidiaries or intermediaries (including distributors, retailers, and others), has committed and continues to commit acts of infringement in this District by, among other things, making, using, importing, offering for sale, and/or selling products and/or services that infringe the patents-in-suit. Thus, Cisco purposefully availed itself of the benefits of doing business in the State of Texas and the exercise of jurisdiction over Cisco would not offend traditional notions of fair play and substantial justice. Cisco is registered to do business in the State of Texas, and has appointed Prentice Hall Corporation System, 211 E. 7th Street, Suite 620, Austin, TX 78701 as its agent for service of process.

11. Venue is proper in this district under 28 U.S.C. §1400(b) and 28 U.S.C. §§ 1391(c). Defendants have regular and established places of business in this district as set forth above.

Count 1 – Claim for infringement of the ’630 patent.

12. Lionra incorporates by reference each of the allegations in paragraphs 1–11 above and further alleges as follows:

13. On March 29, 2011, the United States Patent and Trademark Office issued U.S. Patent No. 7,916,630, entitled “Monitoring Condition of Network with Distributed Components.” Ex. 1.

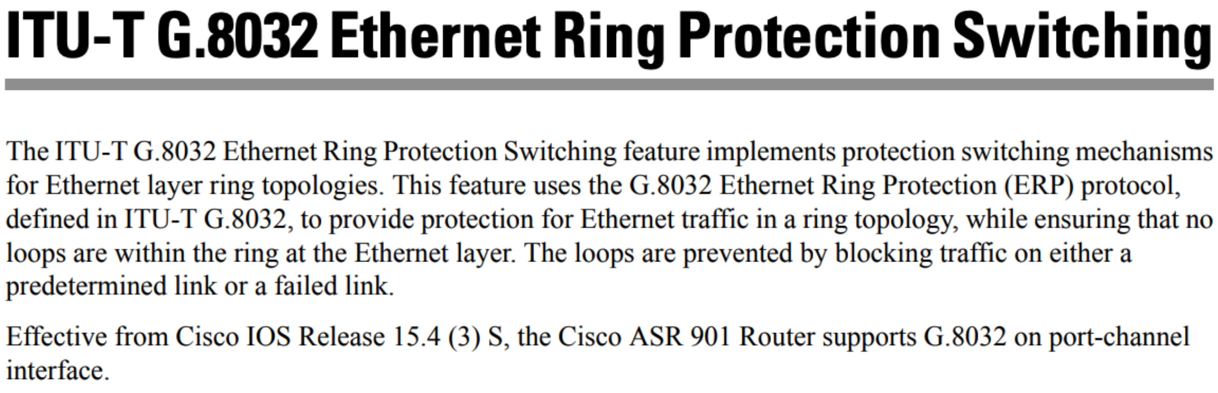
14. Lionra is the owner of the ’630 patent with full rights to pursue recovery of royalties for damages for infringement, including full rights to recover past and future damages.

15. Each claim of the ’630 patent is valid, enforceable, and patent-eligible.

16. Lionra and its predecessors in interest have satisfied the requirements of 35 U.S.C. § 287(a) with respect to the ’630 patent, and Lionra is entitled to damages for Defendant’s past infringement.

17. Defendant has directly infringed (literally and equivalently) and induced others to infringe the ’630 patent by making, using, selling, offering for sale, or importing products that infringe the claims of the ’630 patent and by inducing others to infringe the claims of the ’630 patent without a license or permission from Lionra. These products include without limitation the Cisco ASR 901 Router, which infringes at least claim 1 of the ’630 patent.

18. On information and belief, the ASR 901 performs a method for monitoring a system condition of a network with distributed components organized in a logical ring structure:



ITU-T G.8032 Ethernet Ring Protection Switching

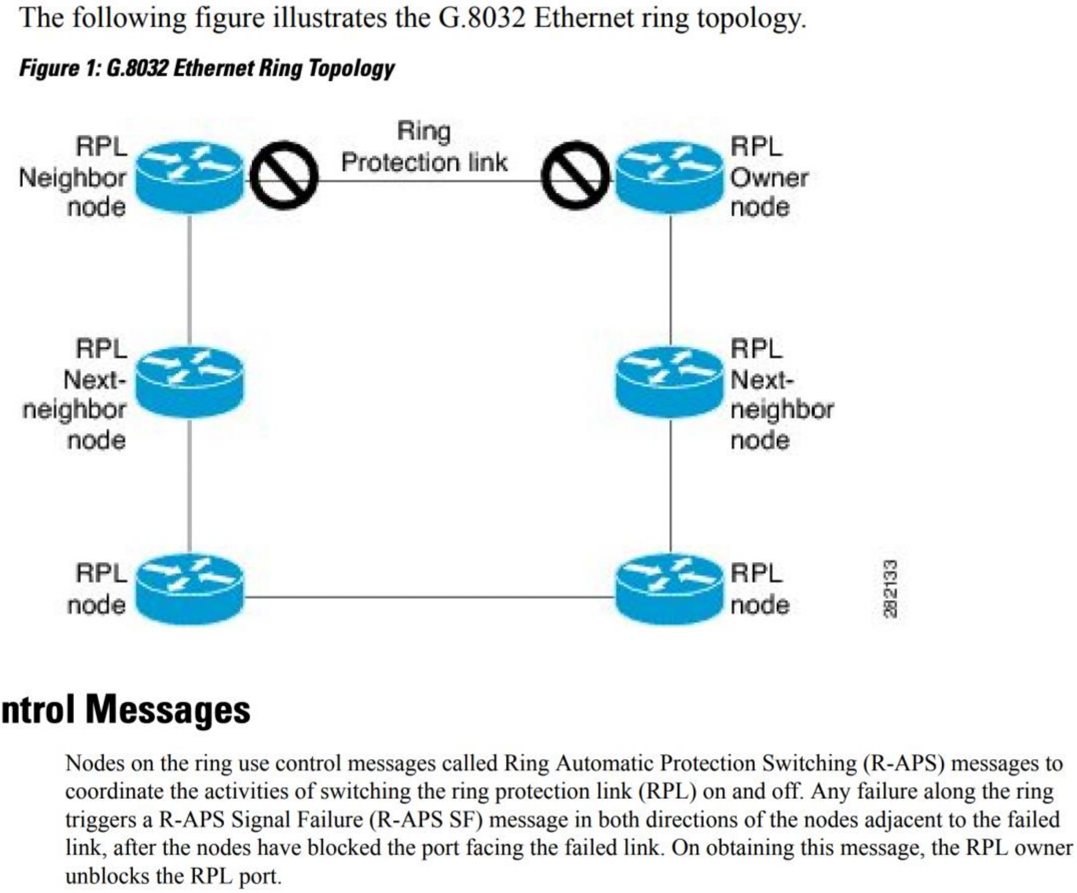
The ITU-T G.8032 Ethernet Ring Protection Switching feature implements protection switching mechanisms for Ethernet layer ring topologies. This feature uses the G.8032 Ethernet Ring Protection (ERP) protocol, defined in ITU-T G.8032, to provide protection for Ethernet traffic in a ring topology, while ensuring that no loops are within the ring at the Ethernet layer. The loops are prevented by blocking traffic on either a predetermined link or a failed link.

Effective from Cisco IOS Release 15.4 (3) S, the Cisco ASR 901 Router supports G.8032 on port-channel interface.

(https://www.cisco.com/c/en/us/td/docs/wireless/asr_901/Configuration/Guide/b_asr901-scg/b_asr901-scg_chapter_0111111.pdf at 1.)

19. On information and belief, in the ASR 901 each component in the system monitors only a single respective neighboring component among said distributed components that is a predecessor

or successor of said each component in the logical ring structure to determine a current condition of the respective neighboring component:



The following figure illustrates the G.8032 Ethernet ring topology.

Figure 1: G.8032 Ethernet Ring Topology

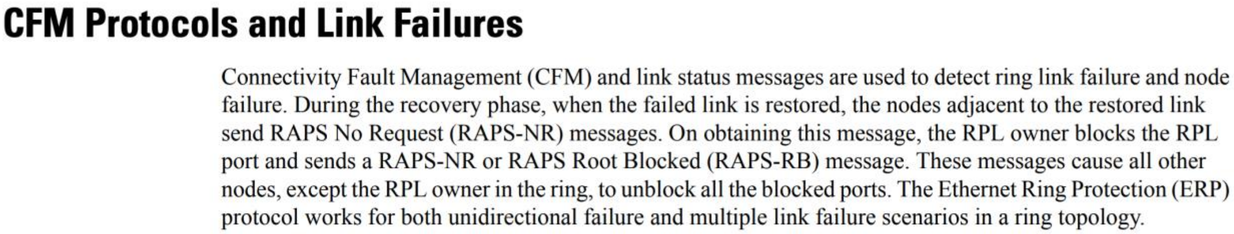
RPL Neighbor node
Ring Protection link
RPL Owner node
RPL Next-neighbor node
RPL Next-neighbor node
RPL node
RPL node
282133

R-APS Control Messages

Nodes on the ring use control messages called Ring Automatic Protection Switching (R-APS) messages to coordinate the activities of switching the ring protection link (RPL) on and off. Any failure along the ring triggers a R-APS Signal Failure (R-APS SF) message in both directions of the nodes adjacent to the failed link, after the nodes have blocked the port facing the failed link. On obtaining this message, the RPL owner unblocks the RPL port.

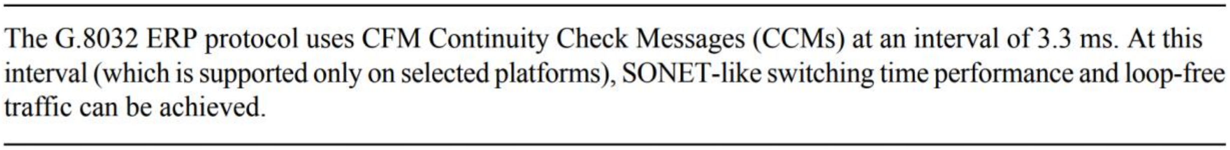
(https://www.cisco.com/c/en/us/td/docs/wireless/asr_901s/scg/b_scg_for_asr901s/b_scg_for_asr901s_chapter_0101011.pdf at 3, 5.)

20. On information and belief, in the ASR 901 each component in the system informs all other components of the system about the current condition of the respective neighboring component when the current condition corresponds to at least one predefined condition:



CFM Protocols and Link Failures

Connectivity Fault Management (CFM) and link status messages are used to detect ring link failure and node failure. During the recovery phase, when the failed link is restored, the nodes adjacent to the restored link send RAPS No Request (RAPS-NR) messages. On obtaining this message, the RPL owner blocks the RPL port and sends a RAPS-NR or RAPS Root Blocked (RAPS-RB) message. These messages cause all other nodes, except the RPL owner in the ring, to unblock all the blocked ports. The Ethernet Ring Protection (ERP) protocol works for both unidirectional failure and multiple link failure scenarios in a ring topology.



The G.8032 ERP protocol uses CFM Continuity Check Messages (CCMs) at an interval of 3.3 ms. At this interval (which is supported only on selected platforms), SONET-like switching time performance and loop-free traffic can be achieved.

(https://www.cisco.com/c/en/us/td/docs/wireless/asr_901s/scg/b_scg_for_asr901s/b_scg_for_asr901s_chapter_0101011.pdf at 6.)

Count 2 – Claim for infringement of the ’612 patent.

21. Lionra incorporates by reference each of the allegations in paragraphs 1–20 above and further alleges as follows:

22. On October 2, 2013, the United States Patent and Trademark Office issued U.S. Patent No. 8,566,612, entitled “System and Method for a Secure I/O Interface.” Ex. 2.

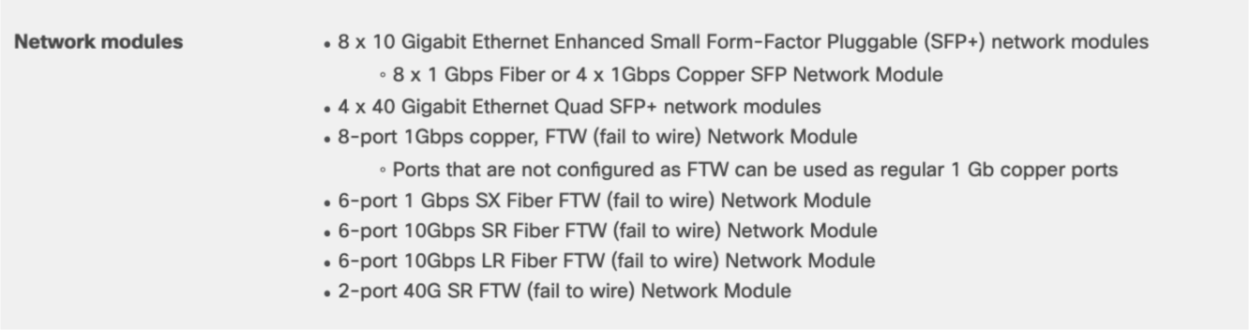
23. Lionra is the owner of the ’612 patent with full rights to pursue recovery of royalties for damages for infringement, including full rights to recover past and future damages.

24. Each claim of the ’612 patent is valid, enforceable, and patent-eligible.

25. Lionra and its predecessors in interest have satisfied the requirements of 35 U.S.C. § 287(a) with respect to the ’612 patent, and Lionra is entitled to damages for Defendant’s past infringement.

26. Defendant has directly infringed (literally and equivalently) and induced others to infringe the ’612 patent by making, using, selling, offering for sale, or importing products that infringe the claims of the ’612 patent and by inducing others to infringe the claims of the ’612 patent without a license or permission from Lionra. These products include without limitation the Cisco Firepower 4100 Series, which infringes at least claim 1 of the ’612 patent.

27. On information and belief, the Cisco Firepower 4100 includes a security processor which includes a switching system to send the outgoing packets and receive the incoming packets:



Network modules	• 8 x 10 Gigabit Ethernet Enhanced Small Form-Factor Pluggable (SFP+) network modules ◦ 8 x 1 Gbps Fiber or 4 x 1Gbps Copper SFP Network Module • 4 x 40 Gigabit Ethernet Quad SFP+ network modules • 8-port 1Gbps copper, FTW (fail to wire) Network Module ◦ Ports that are not configured as FTW can be used as regular 1 Gb copper ports • 6-port 1 Gbps SX Fiber FTW (fail to wire) Network Module • 6-port 10Gbps SR Fiber FTW (fail to wire) Network Module • 6-port 10Gbps LR Fiber FTW (fail to wire) Network Module • 2-port 40G SR FTW (fail to wire) Network Module

(https://www.cisco.com/c/en/us/products/collateral/security/firepower-4100-series/datasheet-c78-742474.html)

28. On information and belief, the Cisco Firepower 4100 includes a packet engine, coupled to the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packets sent by the packet engine to the switching system, wherein the packet engine is one of a plurality of packet engines and substantially all of the incoming and outgoing packets to the security processor transit one of the plurality of packet engines:

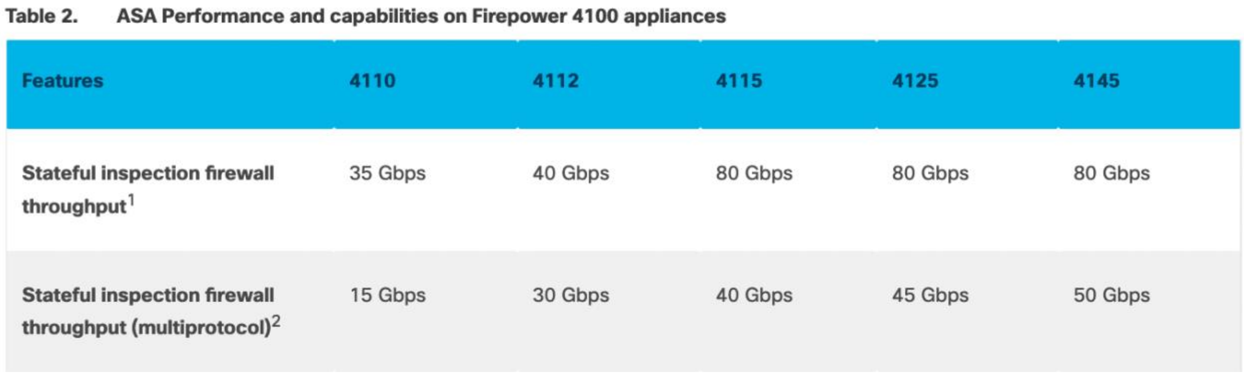
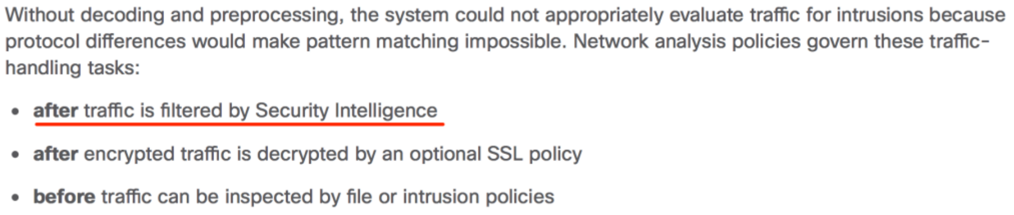


Table 2. ASA Performance and capabilities on Firepower 4100 appliances

Features	4110	4112	4115	4125	4145
Stateful inspection firewall throughput[1]	35 Gbps	40 Gbps	80 Gbps	80 Gbps	80 Gbps
Stateful inspection firewall throughput (multiprotocol)[2]	15 Gbps	30 Gbps	40 Gbps	45 Gbps	50 Gbps

(https://www.cisco.com/c/en/us/products/collateral/security/firepower-4100-series/datasheet-c78-742474.html)

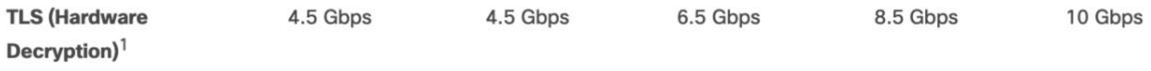


Without decoding and preprocessing, the system could not appropriately evaluate traffic for intrusions because protocol differences would make pattern matching impossible. Network analysis policies govern these traffic-handling tasks:

- **after** traffic is filtered by Security Intelligence
- **after** encrypted traffic is decrypted by an optional SSL policy
- **before** traffic can be inspected by file or intrusion policies

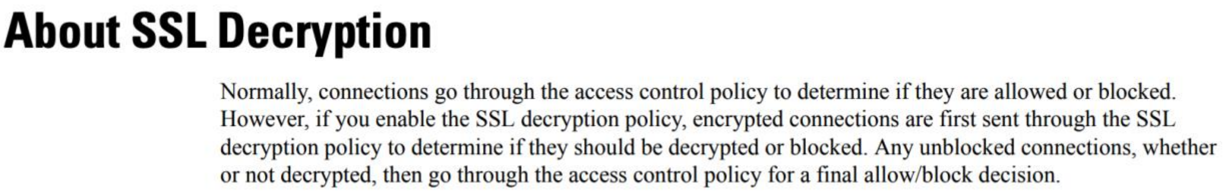
(https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/710/management-center-device-config-71/intrusion-overview.html)

29. On information and belief, the Cisco Firepower 4100 includes a cryptographic core, coupled to the packet engine and receiving the incoming packets from the switching system via the packet engine and communicating the outgoing packets to the switching system via the packet engine, to provide encryption and decryption processing for packets received from and sent to the packet engine, wherein the packet engine is interposed between the switching system and the cryptographic core:



TLS (Hardware Decryption)[1]	4.5 Gbps	4.5 Gbps	6.5 Gbps	8.5 Gbps	10 Gbps

(https://www.cisco.com/c/en/us/products/collateral/security/firepower-4100-series/datasheet-c78-742474.html)

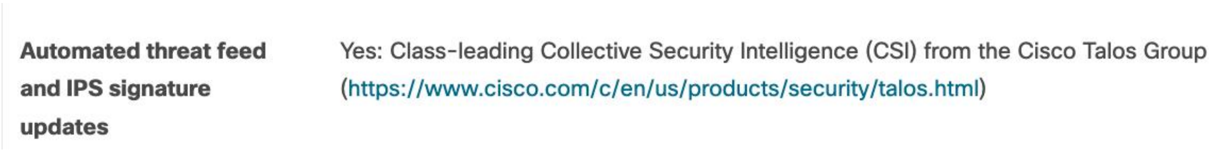


About SSL Decryption

Normally, connections go through the access control policy to determine if they are allowed or blocked. However, if you enable the SSL decryption policy, encrypted connections are first sent through the SSL decryption policy to determine if they should be decrypted or blocked. Any unblocked connections, whether or not decrypted, then go through the access control policy for a final allow/block decision.

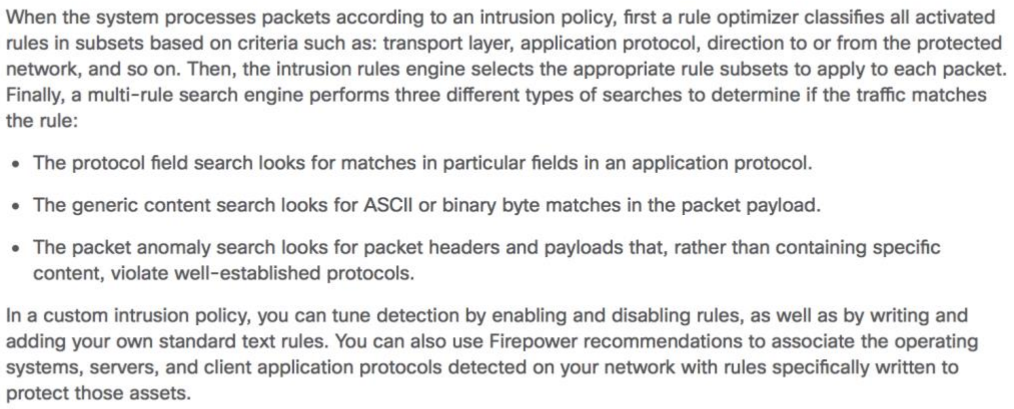
(https://www.cisco.com/c/en/us/td/docs/security/firepower/623/fdm/fptd-fdm-config-guide-623/fptd-fdm-ssl-decryption.pdf at 1.)

30. On information and belief, the Cisco Firepower 4100 includes a signature database:



Automated threat feed and IPS signature updates	Yes: Class-leading Collective Security Intelligence (CSI) from the Cisco Talos Group (https://www.cisco.com/c/en/us/products/security/talos.html)

(https://www.cisco.com/c/en/us/products/collateral/security/firepower-4100-series/datasheet-c78-742474.html)



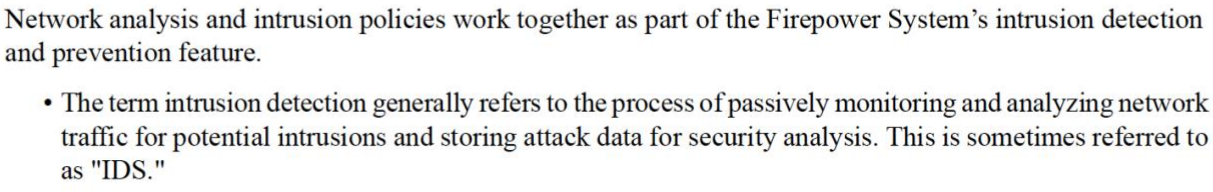
When the system processes packets according to an intrusion policy, first a rule optimizer classifies all activated rules in subsets based on criteria such as: transport layer, application protocol, direction to or from the protected network, and so on. Then, the intrusion rules engine selects the appropriate rule subsets to apply to each packet. Finally, a multi-rule search engine performs three different types of searches to determine if the traffic matches the rule:

- The protocol field search looks for matches in particular fields in an application protocol.
- The generic content search looks for ASCII or binary byte matches in the packet payload.
- The packet anomaly search looks for packet headers and payloads that, rather than containing specific content, violate well-established protocols.

In a custom intrusion policy, you can tune detection by enabling and disabling rules, as well as by writing and adding your own standard text rules. You can also use Firepower recommendations to associate the operating systems, servers, and client application protocols detected on your network with rules specifically written to protect those assets.

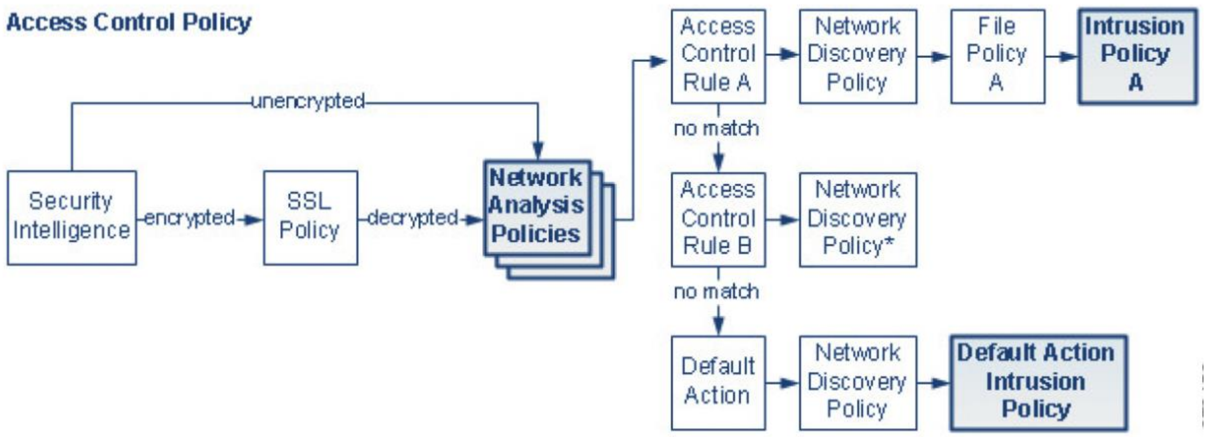
(https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/710/management-center-device-config-71/intrusion-overview.html)

31. On information and belief, the Cisco Firepower 4100 includes an intrusion detection system coupled between the cryptographic core and the packet engine and responsive to at least one packet matching a signature stored in the signature database:

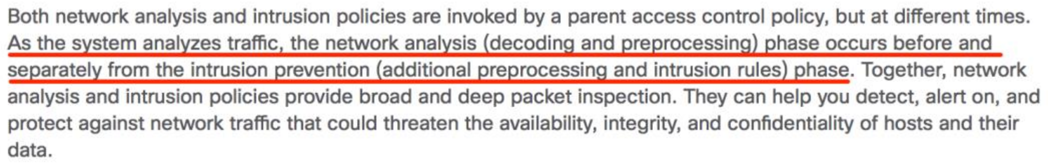


Network analysis and intrusion policies work together as part of the Firepower System's intrusion detection and prevention feature.

- The term intrusion detection generally refers to the process of passively monitoring and analyzing network traffic for potential intrusions and storing attack data for security analysis. This is sometimes referred to as "IDS."



(https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config-guide-v63/overview_of_network_analysis_and_intrusion_policies.pdf at 1, 2.)


Both network analysis and intrusion policies are invoked by a parent access control policy, but at different times. As the system analyzes traffic, the network analysis (decoding and preprocessing) phase occurs before and separately from the intrusion prevention (additional preprocessing and intrusion rules) phase. Together, network analysis and intrusion policies provide broad and deep packet inspection. They can help you detect, alert on, and protect against network traffic that could threaten the availability, integrity, and confidentiality of hosts and their data.

(https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/710/management-center-device-config-71/intrusion-overview.html)

Count 3 – Claim for infringement of the ’323 patent.

32. Lionra incorporates by reference each of the allegations in paragraphs 1–31 above and further alleges as follows:

33. On November 16, 2006, the United States Patent and Trademark Office issued U.S. Patent No. 7,921,323, entitled “Reconfigurable Communications Infrastructure for ASIC Networks.” Ex. 3.

34. Lionra is the owner of the ’323 patent with full rights to pursue recovery of royalties for damages for infringement, including full rights to recover past and future damages.

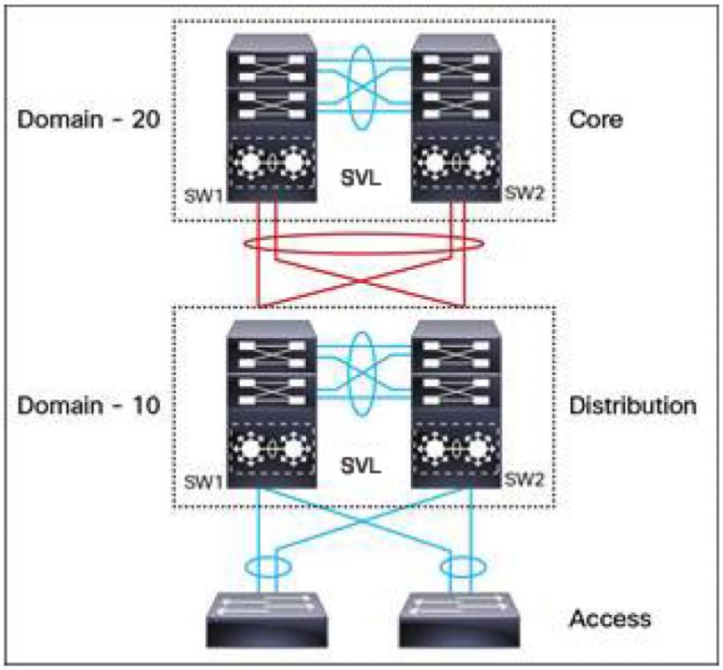
35. Each claim of the ’323 patent is valid, enforceable, and patent-eligible.

36. Lionra and its predecessors in interest have satisfied the requirements of 35 U.S.C. § 287(a) with respect to the ’323 patent, and Lionra is entitled to damages for Defendant’s past infringement.

37. Defendant has directly infringed (literally and equivalently) and induced others to infringe the ’323 patent by making, using, selling, offering for sale, or importing products that infringe the claims of the ’323 patent and by inducing others to infringe the claims of the ’323 patent without a license or permission from Lionra. These products include without limitation the Cisco Catalyst 9500 Series, which infringes at least claim 27 of the ’323 patent.

38. On information and belief, the Cisco Catalyst 9500 is designed and intended for use in a communications infrastructure, comprising two or more separate signal processing circuits:

Figure 1: Typical Network Design using Cisco StackWise Virtual



(https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/16-9/configuration_guide/ha/b_169_ha_9500_cg.pdf at 14.)

39. On information and belief, each one of said two or more signal processing circuits includes multiple ASIC devices that each itself includes a packet router:

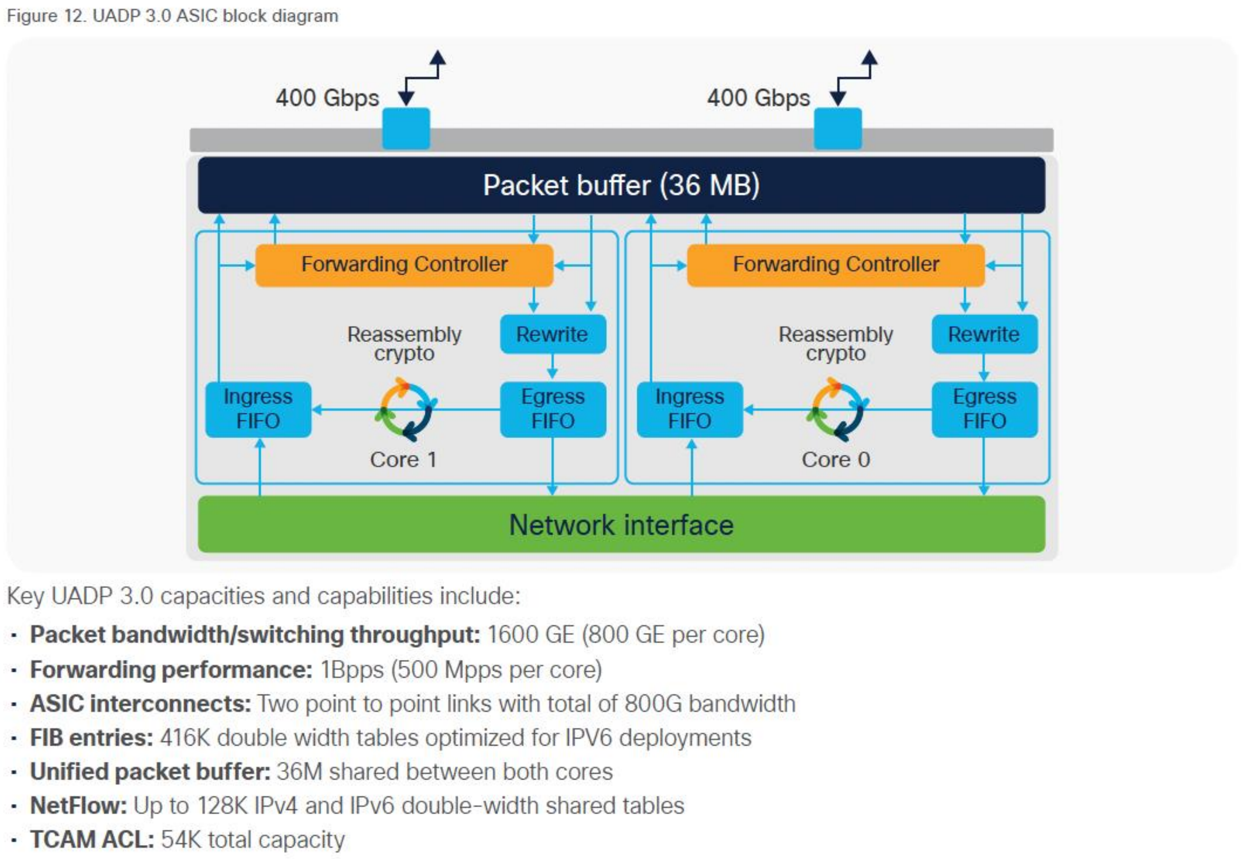
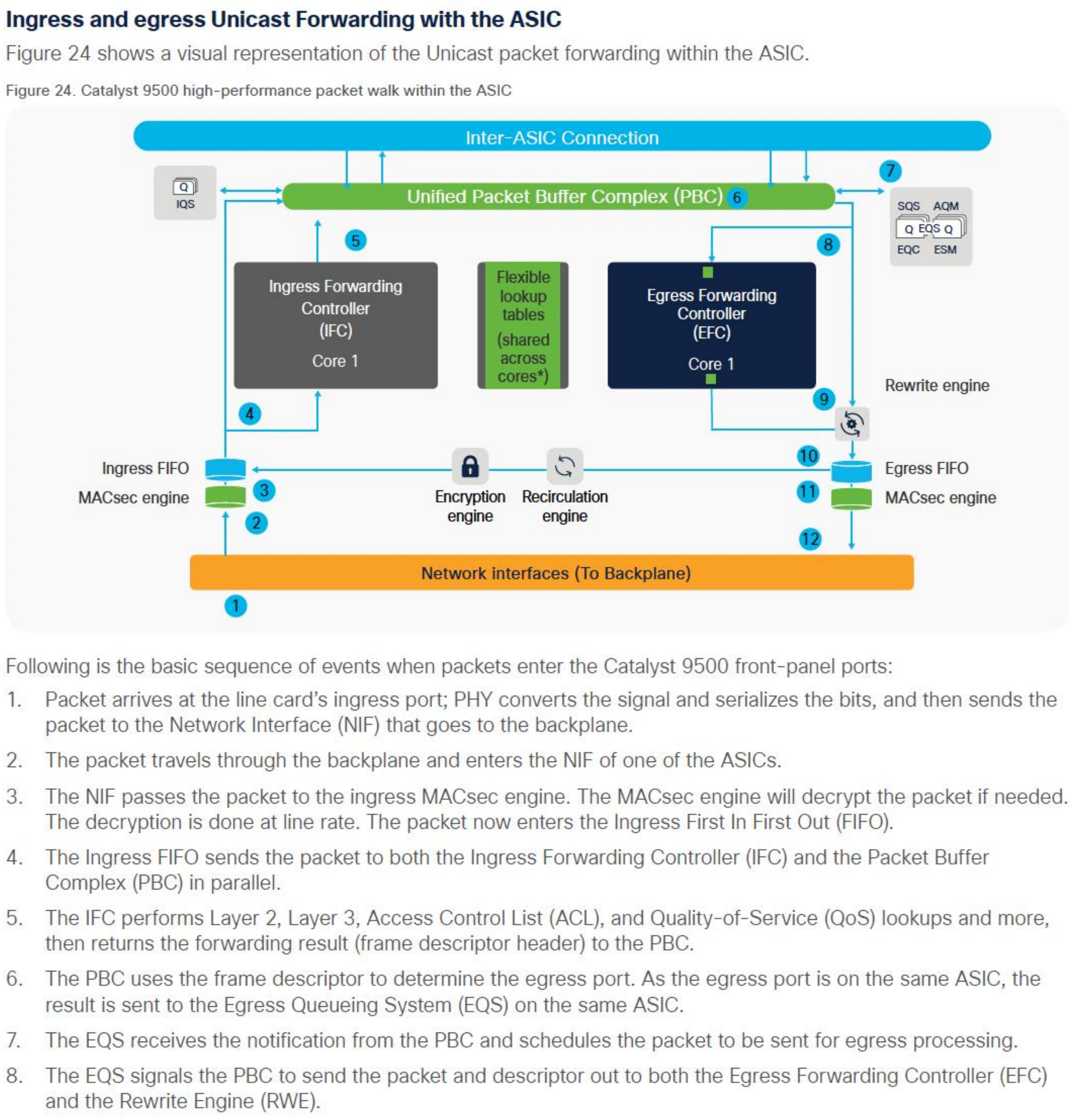


Figure 12. UADP 3.0 ASIC block diagram

Key UADP 3.0 capacities and capabilities include:

- **Packet bandwidth/switching throughput:** 1600 GE (800 GE per core)
- **Forwarding performance:** 1Bpps (500 Mpps per core)
- **ASIC interconnects:** Two point to point links with total of 800G bandwidth
- **FIB entries:** 416K double width tables optimized for IPV6 deployments
- **Unified packet buffer:** 36M shared between both cores
- **NetFlow:** Up to 128K IPv4 and IPv6 double-width shared tables
- **TCAM ACL:** 54K total capacity

(https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9500-series-switches/white-paper-c11-741484.pdf at 11.)


Inter-ASIC Connection
Q
IQS
Unified Packet Buffer Complex (PBC) 6
7
SQS AQM
Q EQS Q
EQC ESM
5
8
Ingress Forwarding Controller (IFC)
Core 1
Flexible lookup tables (shared across cores*)
Egress Forwarding Controller (EFC)
Core 1
Rewrite engine
9
4
10
Ingress FIFO
MACsec engine
3
2
Encryption engine
Recirculation engine
11
Egress FIFO
MACsec engine
12
Network interfaces (To Backplane)
1

Ingress and egress Unicast Forwarding with the ASIC

Figure 24 shows a visual representation of the Unicast packet forwarding within the ASIC.

Figure 24. Catalyst 9500 high-performance packet walk within the ASIC

Following is the basic sequence of events when packets enter the Catalyst 9500 front-panel ports:

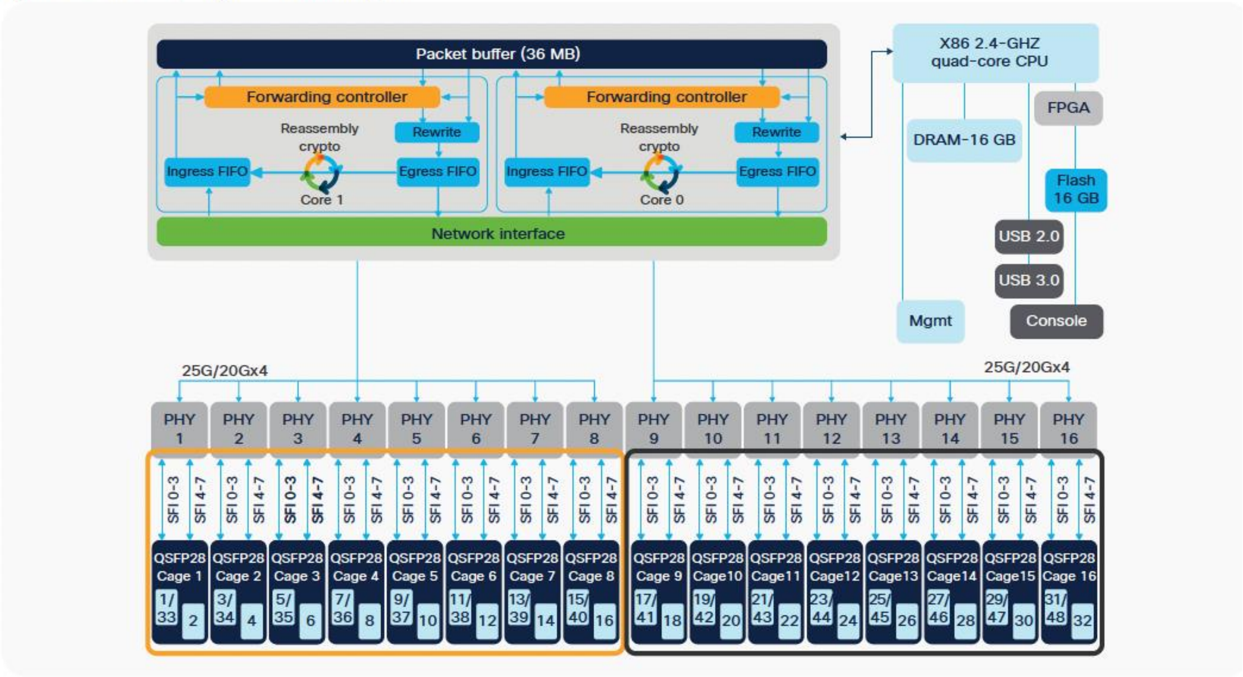
1. Packet arrives at the line card's ingress port; PHY converts the signal and serializes the bits, and then sends the packet to the Network Interface (NIF) that goes to the backplane.
2. The packet travels through the backplane and enters the NIF of one of the ASICs.
3. The NIF passes the packet to the ingress MACsec engine. The MACsec engine will decrypt the packet if needed. The decryption is done at line rate. The packet now enters the Ingress First In First Out (FIFO).
4. The Ingress FIFO sends the packet to both the Ingress Forwarding Controller (IFC) and the Packet Buffer Complex (PBC) in parallel.
5. The IFC performs Layer 2, Layer 3, Access Control List (ACL), and Quality-of-Service (QoS) lookups and more, then returns the forwarding result (frame descriptor header) to the PBC.
6. The PBC uses the frame descriptor to determine the egress port. As the egress port is on the same ASIC, the result is sent to the Egress Queueing System (EQS) on the same ASIC.
7. The EQS receives the notification from the PBC and schedules the packet to be sent for egress processing.
8. The EQS signals the PBC to send the packet and descriptor out to both the Egress Forwarding Controller (EFC) and the Rewrite Engine (RWE).

(https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9500-series-switches/white-paper-c11-741484.pdf at 22.)

40. On information and belief, said packet router of each one of said ASIC devices of each given one of said respective two or more signal processing circuits being coupled through respective first and second common interfaces and an intervening high speed serial optical link to a respective packet router of each of the ASIC devices of each other of said two or more signal

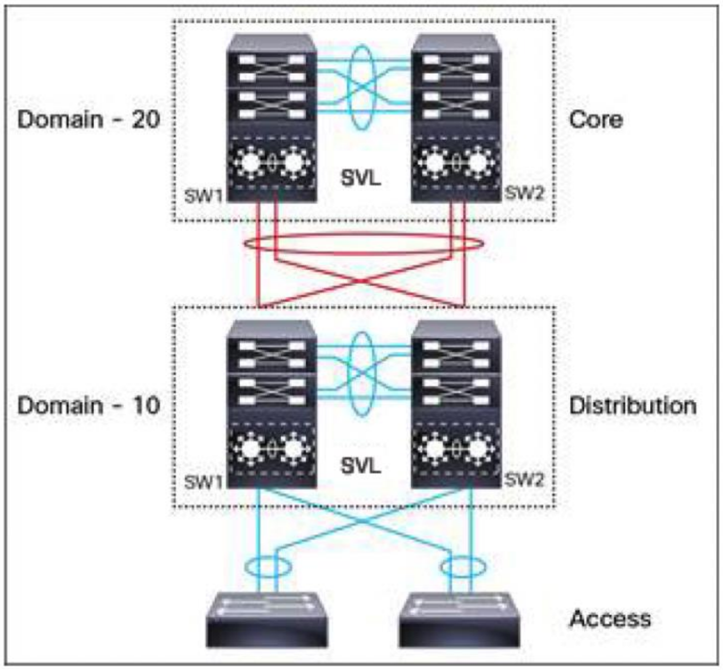
processing circuits with no other processing device intervening between the high speed optical link and said ASIC devices of each of said two or more signal processing circuits:

Figure 17. C9500-32QC high-level block diagram



(https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9500-series-switches/white-paper-c11-741484.pdf at 15.)

Figure 1: Typical Network Design using Cisco StackWise Virtual



(https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/16-9/configuration_guide/ha/b_169_ha_9500_cg.pdf at 14.)

Count 4 – Claim for infringement of the ’708 patent.

41. Lionra incorporates by reference each of the allegations in paragraphs 1–40 above and further alleges as follows:

42. On November 27, 2007, the United States Patent and Trademark Office issued U.S. Patent No. 7,302,708, entitled “Enforcing Computer Security Utilizing an Adaptive Lattice Mechanism.” Ex. 4.

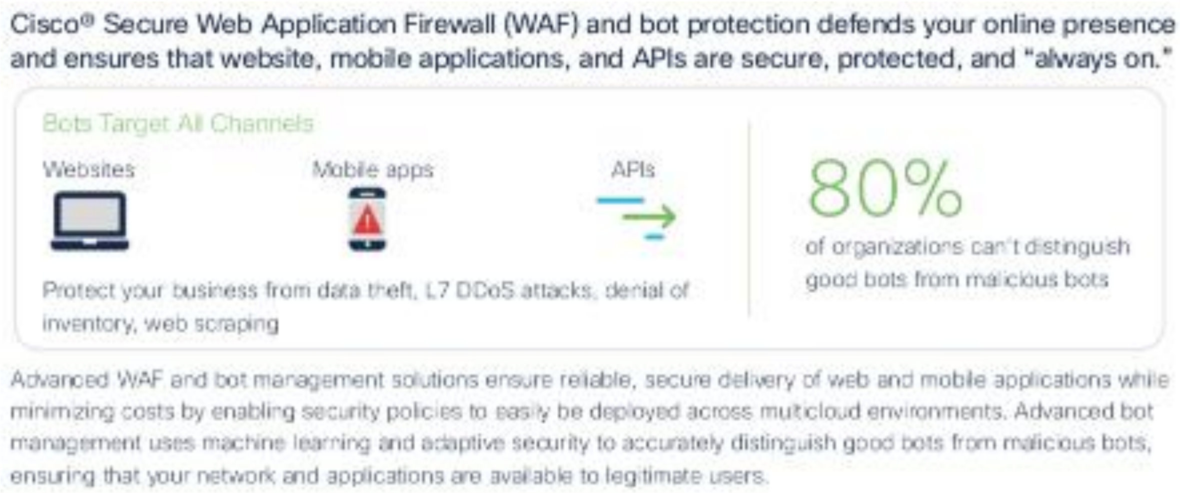
43. Lionra is the owner of the ’708 patent with full rights to pursue recovery of royalties for damages for infringement, including full rights to recover past and future damages.

44. Each claim of the ’708 patent is valid, enforceable, and patent-eligible.

45. Lionra and its predecessors in interest have satisfied the requirements of 35 U.S.C. § 287(a) with respect to the ’708 patent, and Lionra is entitled to damages for Defendant’s past infringement.

46. Defendant has directly infringed (literally and equivalently) and induced others to infringe the ’708 patent by making, using, selling, offering for sale, or importing products that infringe the claims of the ’708 patent and by inducing others to infringe the claims of the ’708 patent without a license or permission from Lionra. These products include without limitation the Cisco Secure Web Application Firewall, which infringes at least claim 1 of the ’708 patent.

47. On information and belief, the Secure Web Application Firewall performs a method for secure access to a computer system:



Cisco® Secure Web Application Firewall (WAF) and bot protection defends your online presence and ensures that website, mobile applications, and APIs are secure, protected, and “always on.”

Bots Target All Channels

Websites

Mobile apps

APIs

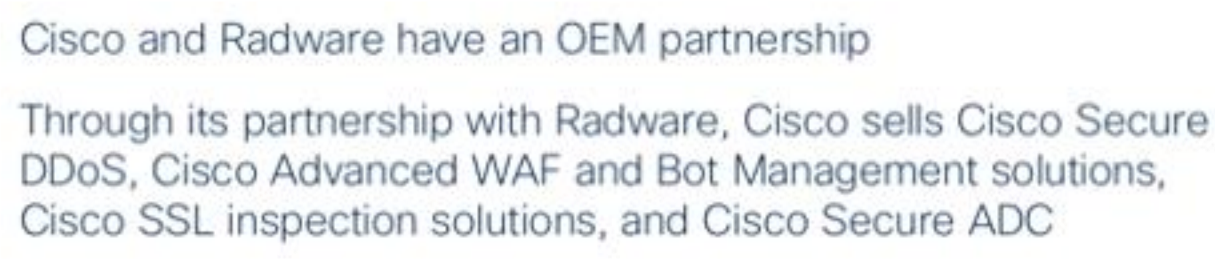
Protect your business from data theft, L7 DDoS attacks, denial of inventory, web scraping

80%

of organizations can’t distinguish good bots from malicious bots

Advanced WAF and bot management solutions ensure reliable, secure delivery of web and mobile applications while minimizing costs by enabling security policies to easily be deployed across multicloud environments. Advanced bot management uses machine learning and adaptive security to accurately distinguish good bots from malicious bots, ensuring that your network and applications are available to legitimate users.

(https://www.cisco.com/c/en/us/products/collateral/security/advanced-waf-bot-aag.pdf)

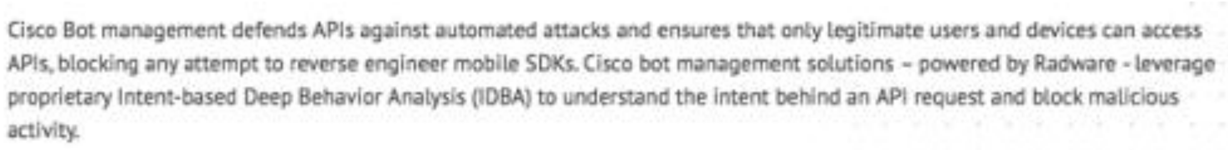


Cisco and Radware have an OEM partnership

Through its partnership with Radware, Cisco sells Cisco Secure DDoS, Cisco Advanced WAF and Bot Management solutions, Cisco SSL inspection solutions, and Cisco Secure ADC

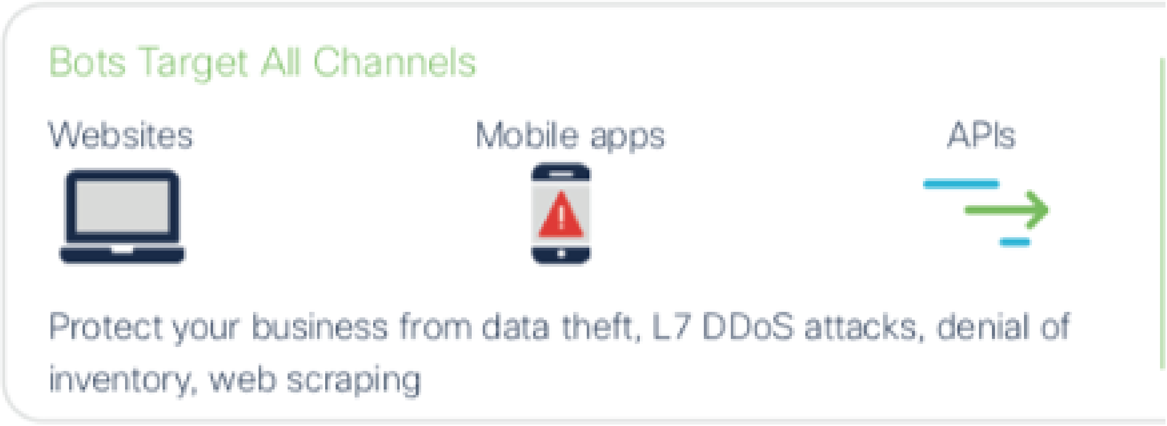
(https://www.cisco.com/c/dam/en/us/products/collateral/security/secure-ddos-services.pdf)

48. On information and belief, the Secure Web Application Firewall receives in the computer system a request from an entity with a predetermined access level for access to a first base node representing at least one of an information type and a computer system function:



Cisco Bot management defends APIs against automated attacks and ensures that only legitimate users and devices can access APIs, blocking any attempt to reverse engineer mobile SDKs. Cisco bot management solutions – powered by Radware - leverage proprietary Intent-based Deep Behavior Analysis (IDBA) to understand the intent behind an API request and block malicious activity.

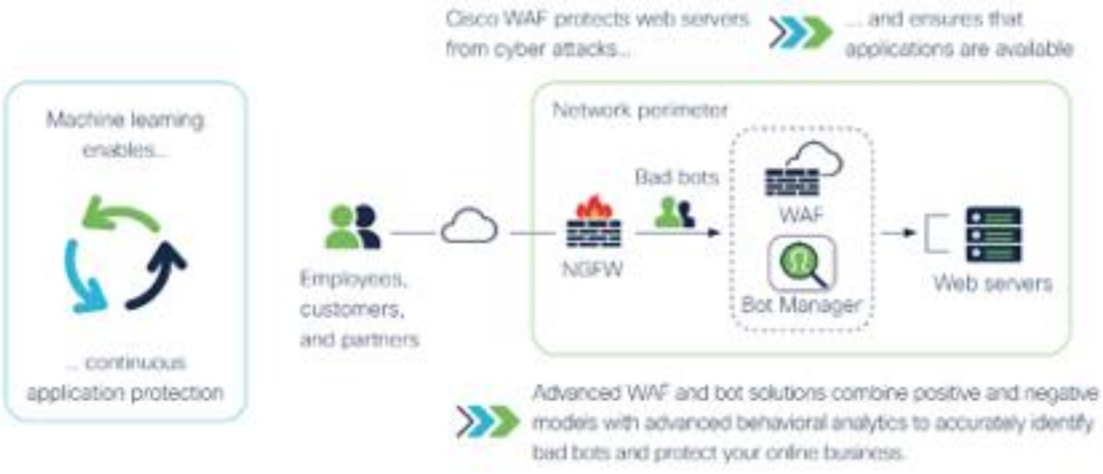
(https://www.radware.com/partners/cisco-waf-bot/)



Bots Target All Channels

Protect your business from data theft, L7 DDoS attacks, denial of inventory, web scraping

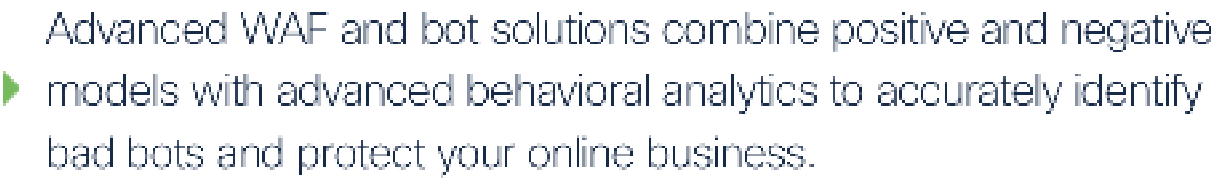
(https://www.cisco.com/c/en/us/products/collateral/security/advanced-waf-bot-aag.pdf)



Cisco WAF protects web servers from cyber attacks...
...and ensures that applications are available
Machine learning enables...
...continuous application protection
Employees, customers, and partners
Network perimeter
Bad bots
NGFW
WAF
Bot Manager
Web servers
Advanced WAF and bot solutions combine positive and negative models with advanced behavioral analytics to accurately identify bad bots and protect your online business

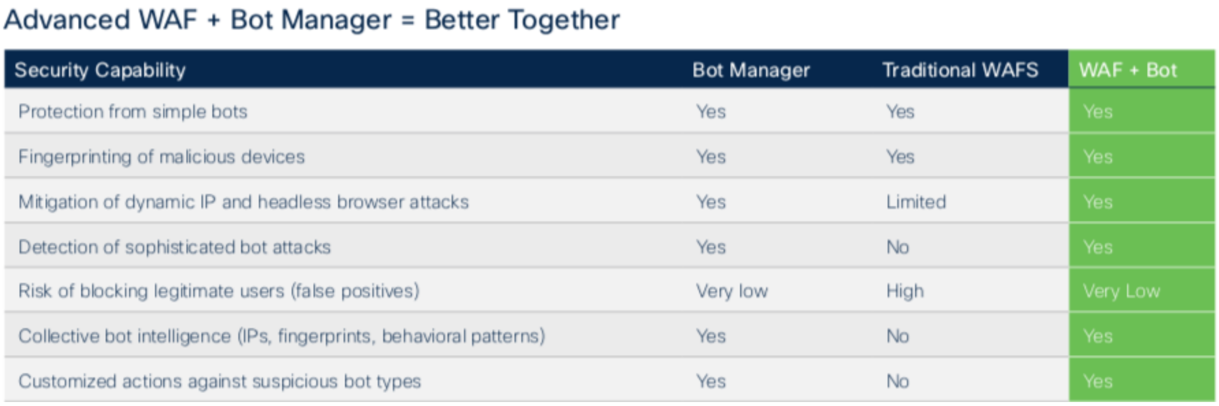
(https://www.cisco.com/c/en/us/products/collateral/security/advanced-waf-bot-aag.pdf)

49. On information and belief, the Secure Web Application Firewall determines if the access request completes a prohibited temporal access pattern for the entity:



Advanced WAF and bot solutions combine positive and negative models with advanced behavioral analytics to accurately identify bad bots and protect your online business.

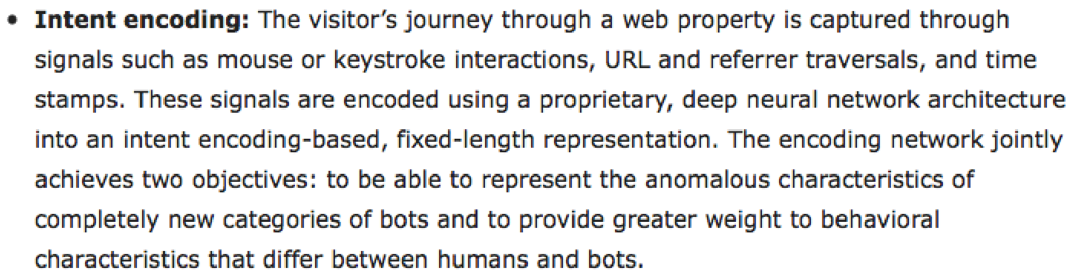
(https://www.cisco.com/c/en/us/products/collateral/security/advanced-waf-bot-aag.pdf)



Advanced WAF + Bot Manager = Better Together

Security Capability	Bot Manager	Traditional WAFS	WAF + Bot
Protection from simple bots	Yes	Yes	Yes
Fingerprinting of malicious devices	Yes	Yes	Yes
Mitigation of dynamic IP and headless browser attacks	Yes	Limited	Yes
Detection of sophisticated bot attacks	Yes	No	Yes
Risk of blocking legitimate users (false positives)	Very low	High	Very Low
Collective bot intelligence (IPs, fingerprints, behavioral patterns)	Yes	No	Yes
Customized actions against suspicious bot types	Yes	No	Yes

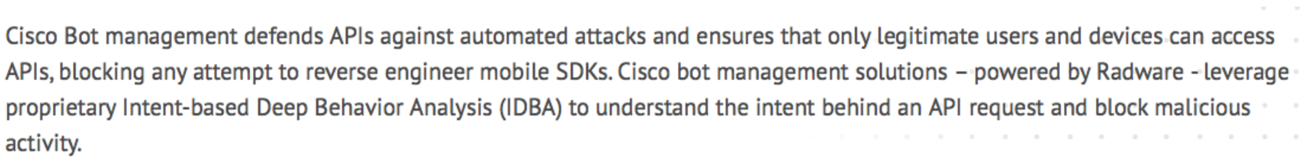
(https://www.cisco.com/c/en/us/products/collateral/security/advanced-waf-bot-aag.pdf)



- **Intent encoding:** The visitor's journey through a web property is captured through signals such as mouse or keystroke interactions, URL and referrer traversals, and time stamps. These signals are encoded using a proprietary, deep neural network architecture into an intent encoding-based, fixed-length representation. The encoding network jointly achieves two objectives: to be able to represent the anomalous characteristics of completely new categories of bots and to provide greater weight to behavioral characteristics that differ between humans and bots.

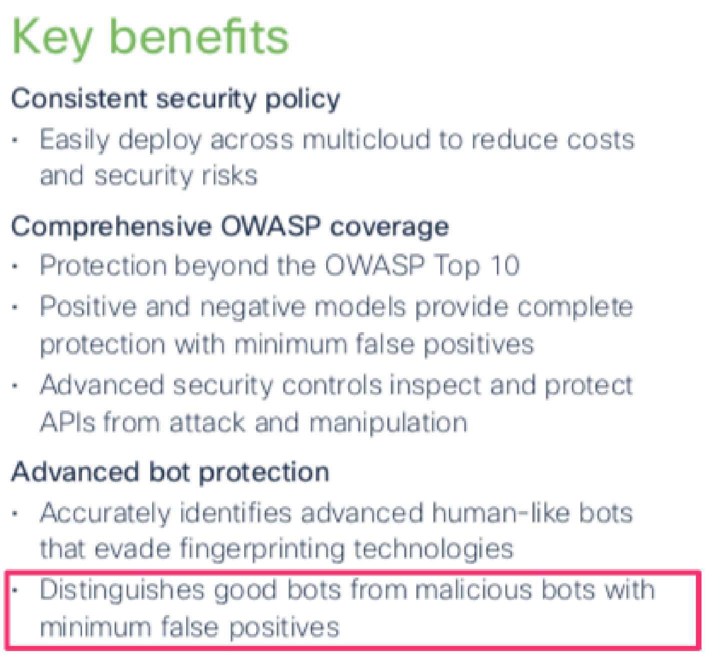
(https://blog.radware.com/security/2019/06/idba-a-patented-bot-detection-technology/)

50. On information and belief, the Secure Web Application Firewall compares a minimum access level established for the first base node to the predetermined access level:



Cisco Bot management defends APIs against automated attacks and ensures that only legitimate users and devices can access APIs, blocking any attempt to reverse engineer mobile SDKs. Cisco bot management solutions – powered by Radware - leverage proprietary Intent-based Deep Behavior Analysis (IDBA) to understand the intent behind an API request and block malicious activity.

(https://www.radware.com/partners/cisco-waf-bot/)



Key benefits

Consistent security policy

- Easily deploy across multicloud to reduce costs and security risks

Comprehensive OWASP coverage

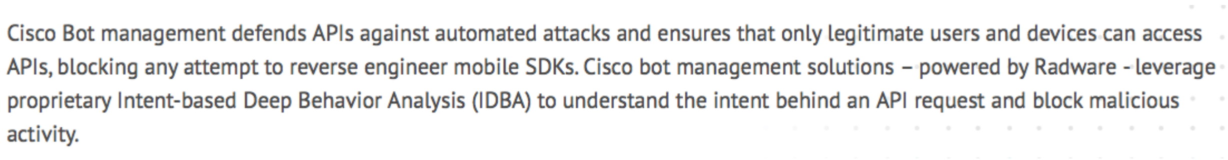
- Protection beyond the OWASP Top 10
- Positive and negative models provide complete protection with minimum false positives
- Advanced security controls inspect and protect APIs from attack and manipulation

Advanced bot protection

- Accurately identifies advanced human-like bots that evade fingerprinting technologies
- Distinguishes good bots from malicious bots with minimum false positives

(https://www.cisco.com/c/en/us/products/collateral/security/advanced-waf-bot-aag.pdf)

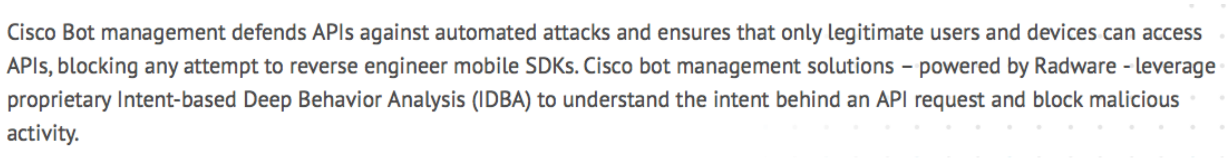
51. On information and belief, the Secure Web Application Firewall grants the access request only if it does not complete a prohibited temporal access pattern for the entity and the minimum access level for the first base node does not exceed the predetermined access level:



Cisco Bot management defends APIs against automated attacks and ensures that only legitimate users and devices can access APIs, blocking any attempt to reverse engineer mobile SDKs. Cisco bot management solutions – powered by Radware - leverage proprietary Intent-based Deep Behavior Analysis (IDBA) to understand the intent behind an API request and block malicious activity.

(https://www.radware.com/partners/cisco-waf-bot/)

52. On information and belief, the Secure Web Application Firewall denies the request if the access request completes a prohibited temporal access pattern for the entity:



Cisco Bot management defends APIs against automated attacks and ensures that only legitimate users and devices can access APIs, blocking any attempt to reverse engineer mobile SDKs. Cisco bot management solutions – powered by Radware - leverage proprietary Intent-based Deep Behavior Analysis (IDBA) to understand the intent behind an API request and block malicious activity.

(https://www.radware.com/partners/cisco-waf-bot/)

Count 5 – Claim for infringement of the ’436 patent.

53. Lionra incorporates by reference each of the allegations in paragraphs 1–52 above and further alleges as follows:

54. On March 23, 2010, the United States Patent and Trademark Office issued U.S. Patent No. 7,685,436, entitled “System and Method for a Secure I/O Interface.” Ex. 5.

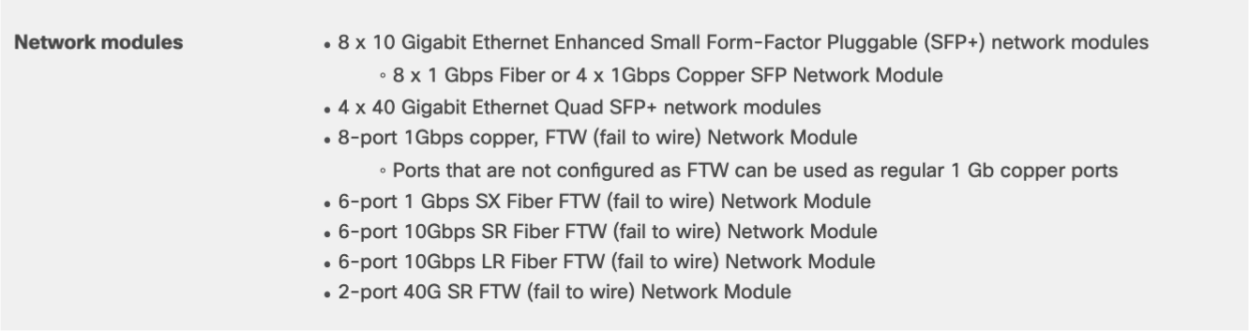
55. Lionra is the owner of the ’436 patent with full rights to pursue recovery of royalties for damages for infringement, including full rights to recover past and future damages.

56. Each claim of the ’436 patent is valid, enforceable, and patent-eligible.

57. Lionra and its predecessors in interest have satisfied the requirements of 35 U.S.C. § 287(a) with respect to the ’436 patent, and Lionra is entitled to damages for Defendant’s past infringement.

58. Defendant has directly infringed (literally and equivalently) and induced others to infringe the ’436 patent by making, using, selling, offering for sale, or importing products that infringe the claims of the ’436 patent and by inducing others to infringe the claims of the ’436 patent without a license or permission from Lionra. These products include without limitation the Cisco Firepower 4100, which infringes at least claim 1 of the ’436 patent.

59. On information and belief, the Cisco Firepower 4100 includes a security processor which includes a switching system to send the outgoing packets and receive the incoming packets:

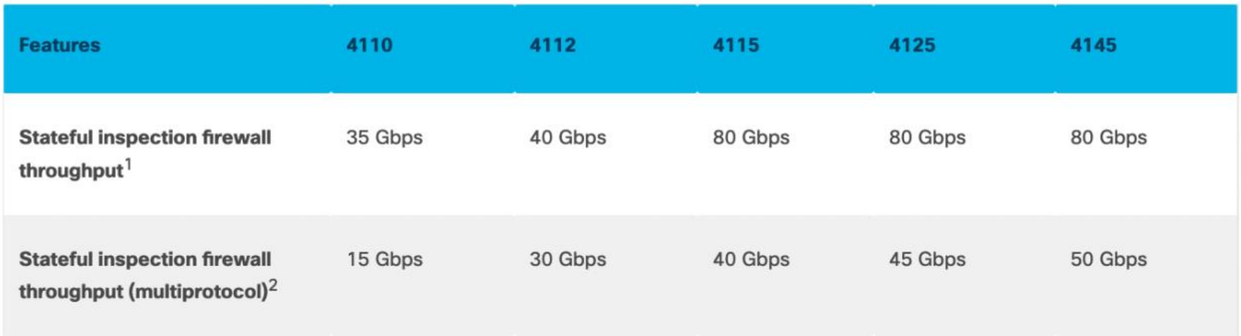


Network modules	• 8 x 10 Gigabit Ethernet Enhanced Small Form-Factor Pluggable (SFP+) network modules ◦ 8 x 1 Gbps Fiber or 4 x 1Gbps Copper SFP Network Module • 4 x 40 Gigabit Ethernet Quad SFP+ network modules • 8-port 1Gbps copper, FTW (fail to wire) Network Module ◦ Ports that are not configured as FTW can be used as regular 1 Gb copper ports • 6-port 1 Gbps SX Fiber FTW (fail to wire) Network Module • 6-port 10Gbps SR Fiber FTW (fail to wire) Network Module • 6-port 10Gbps LR Fiber FTW (fail to wire) Network Module • 2-port 40G SR FTW (fail to wire) Network Module

(https://www.cisco.com/c/en/us/products/collateral/security/firepower-4100-series/datasheet-c78-742474.html)

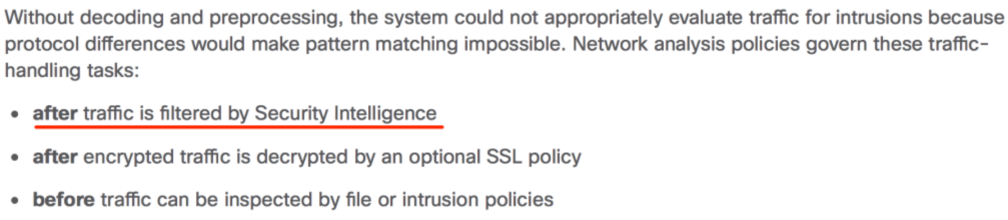
60. On information and belief, the Cisco Firepower 4100 includes a packet engine, coupled to the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packets sent by the packet engine to the switching system, wherein the packet engine is one of a plurality of packet engines and substantially all of the incoming and outgoing packets to the security processor transit one of the plurality of packet engines:

Table 2. ASA Performance and capabilities on Firepower 4100 appliances



Features	4110	4112	4115	4125	4145
Stateful inspection firewall throughput[1]	35 Gbps	40 Gbps	80 Gbps	80 Gbps	80 Gbps
Stateful inspection firewall throughput (multiprotocol)[2]	15 Gbps	30 Gbps	40 Gbps	45 Gbps	50 Gbps

(https://www.cisco.com/c/en/us/products/collateral/security/firepower-4100-series/datasheet-c78-742474.html)

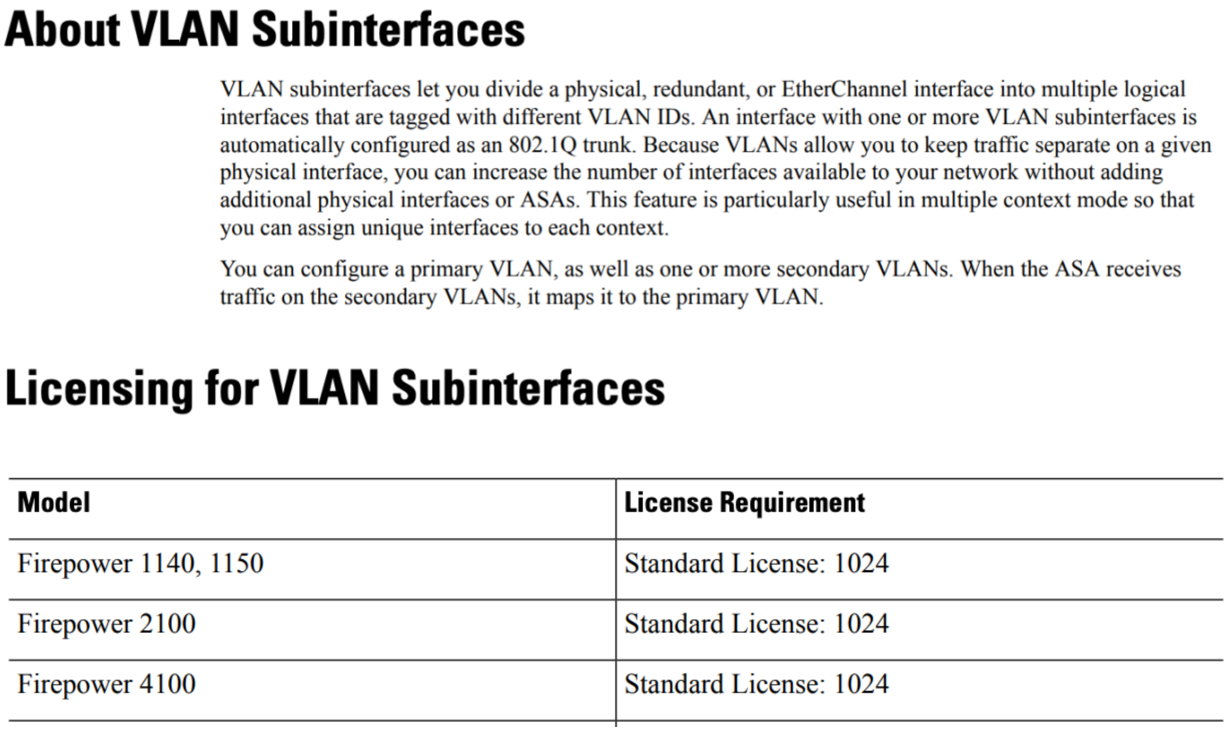


Without decoding and preprocessing, the system could not appropriately evaluate traffic for intrusions because protocol differences would make pattern matching impossible. Network analysis policies govern these traffic-handling tasks:

- **after** traffic is filtered by Security Intelligence
- **after** encrypted traffic is decrypted by an optional SSL policy
- **before** traffic can be inspected by file or intrusion policies

(https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/710/management-center-device-config-71/intrusion-overview.html)

61. On information and belief, the Cisco Firepower 4100 provides the incoming packets and outgoing packets with a tag upon ingress to one of the plurality of packet engines and the tag determines an egress path within the security processor upon exit from a corresponding cryptographic core:



About VLAN Subinterfaces

VLAN subinterfaces let you divide a physical, redundant, or EtherChannel interface into multiple logical interfaces that are tagged with different VLAN IDs. An interface with one or more VLAN subinterfaces is automatically configured as an 802.1Q trunk. Because VLANs allow you to keep traffic separate on a given physical interface, you can increase the number of interfaces available to your network without adding additional physical interfaces or ASAs. This feature is particularly useful in multiple context mode so that you can assign unique interfaces to each context.

You can configure a primary VLAN, as well as one or more secondary VLANs. When the ASA receives traffic on the secondary VLANs, it maps it to the primary VLAN.

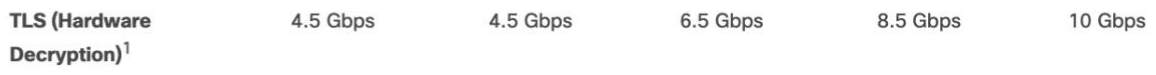
Licensing for VLAN Subinterfaces

Model	License Requirement
Firepower 1140, 1150	Standard License: 1024
Firepower 2100	Standard License: 1024
Firepower 4100	Standard License: 1024

(https://www.cisco.com/c/en/us/td/docs/security/asa/asa914/configuration/general/asa-914-general-config/interface-vlan.pdf at 1, 2.)

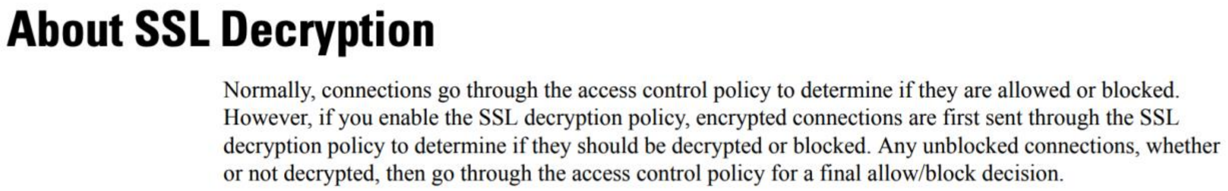
62. On information and belief, the Cisco Firepower 4100 includes a cryptographic core, coupled to the packet engine and receiving the incoming packets from the switching system via

the packet engine and communicating the outgoing packets to the switching system via the packet engine, to provide encryption and decryption processing for packets received from and sent to the packet engine, wherein the packet engine is interposed between the switching system and the cryptographic core:



TLS (Hardware Decryption)[1]	4.5 Gbps	4.5 Gbps	6.5 Gbps	8.5 Gbps	10 Gbps

(https://www.cisco.com/c/en/us/products/collateral/security/firepower-4100-series/datasheet-c78-742474.html)

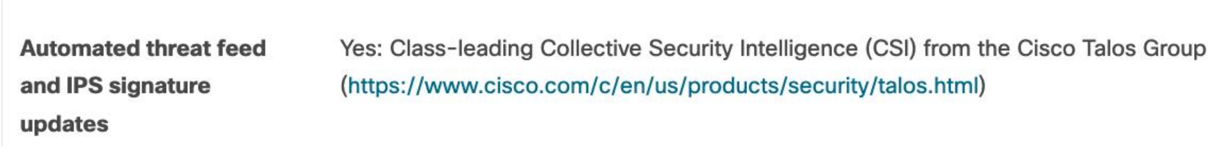


About SSL Decryption

Normally, connections go through the access control policy to determine if they are allowed or blocked. However, if you enable the SSL decryption policy, encrypted connections are first sent through the SSL decryption policy to determine if they should be decrypted or blocked. Any unblocked connections, whether or not decrypted, then go through the access control policy for a final allow/block decision.

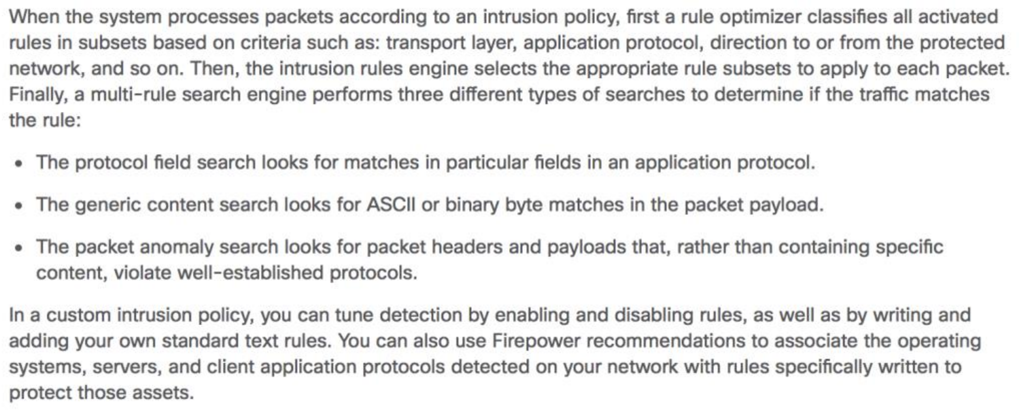
(https://www.cisco.com/c/en/us/td/docs/security/firepower/623/fdm/fptd-fdm-config-guide-623/fptd-fdm-ssl-decryption.pdf at 1.)

63. On information and belief, the Cisco Firepower 4100 includes a signature database:



Automated threat feed and IPS signature updates	Yes: Class-leading Collective Security Intelligence (CSI) from the Cisco Talos Group (https://www.cisco.com/c/en/us/products/security/talos.html)

(https://www.cisco.com/c/en/us/products/collateral/security/firepower-4100-series/datasheet-c78-742474.html)



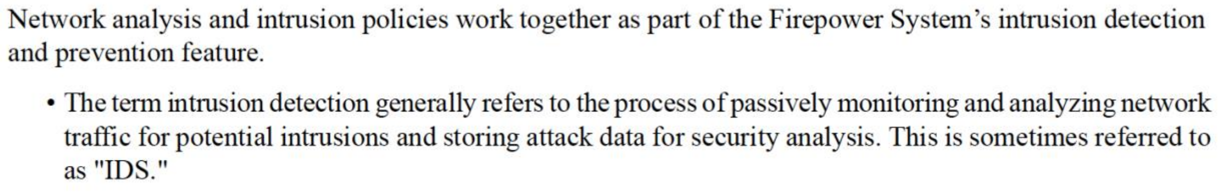
When the system processes packets according to an intrusion policy, first a rule optimizer classifies all activated rules in subsets based on criteria such as: transport layer, application protocol, direction to or from the protected network, and so on. Then, the intrusion rules engine selects the appropriate rule subsets to apply to each packet. Finally, a multi-rule search engine performs three different types of searches to determine if the traffic matches the rule:

- The protocol field search looks for matches in particular fields in an application protocol.
- The generic content search looks for ASCII or binary byte matches in the packet payload.
- The packet anomaly search looks for packet headers and payloads that, rather than containing specific content, violate well-established protocols.

In a custom intrusion policy, you can tune detection by enabling and disabling rules, as well as by writing and adding your own standard text rules. You can also use Firepower recommendations to associate the operating systems, servers, and client application protocols detected on your network with rules specifically written to protect those assets.

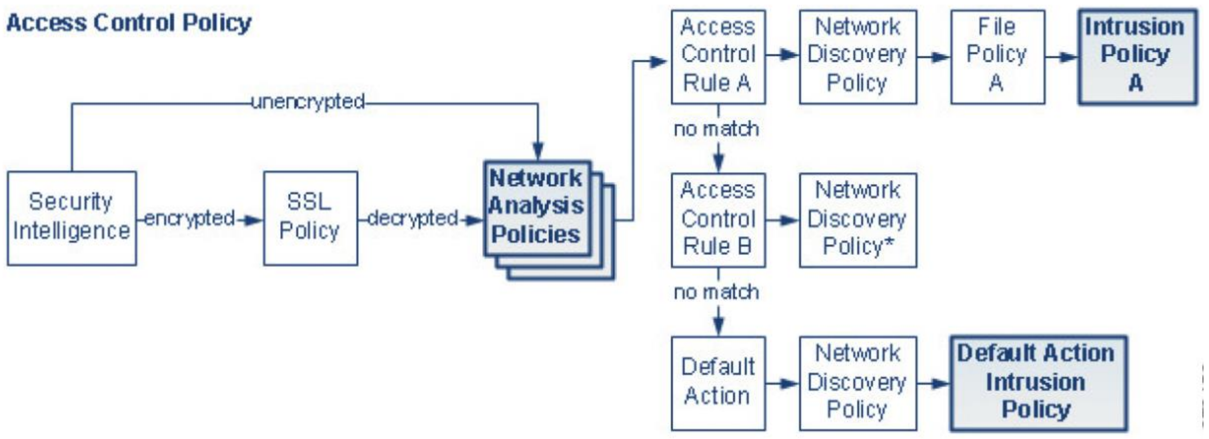
(https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/710/management-center-device-config-71/intrusion-overview.html)

64. On information and belief, the Cisco Firepower 4100 includes an intrusion detection system coupled between the cryptographic core and the packet engine and responsive to at least one packet matching a signature stored in the signature database:

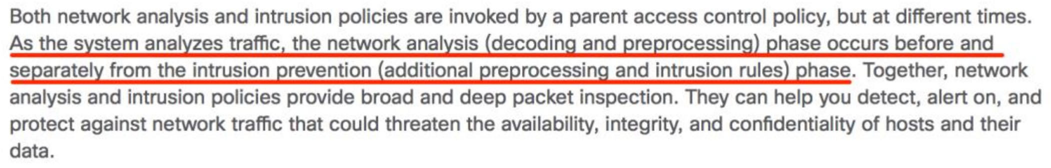


Network analysis and intrusion policies work together as part of the Firepower System's intrusion detection and prevention feature.

- The term intrusion detection generally refers to the process of passively monitoring and analyzing network traffic for potential intrusions and storing attack data for security analysis. This is sometimes referred to as "IDS."



(https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config-guide-v63/overview_of_network_analysis_and_intrusion_policies.pdf at 1, 2.)



Both network analysis and intrusion policies are invoked by a parent access control policy, but at different times. As the system analyzes traffic, the network analysis (decoding and preprocessing) phase occurs before and separately from the intrusion prevention (additional preprocessing and intrusion rules) phase. Together, network analysis and intrusion policies provide broad and deep packet inspection. They can help you detect, alert on, and protect against network traffic that could threaten the availability, integrity, and confidentiality of hosts and their data.

(https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/710/management-center-device-config-71/intrusion-overview.html)

Jury Trial Demanded

65. Pursuant to Rule 38 of the Federal Rules of Civil Procedure, Lionra requests a trial by jury of any issues so triable by right.

Prayer for Relief

Plaintiff Lionra respectfully requests the following relief from this Court:

A. A judgment in favor of Lionra that Defendant has infringed the ’630, ’612, ’323, ’708, and ’436 patents, and that the ’630, ’612, ’323, ’708, and ’436 patents are valid, enforceable, and patent-eligible;

B. A judgment and order requiring Defendant to pay Lionra compensatory damages, costs, expenses, and pre- and post-judgment interest for its infringement of the asserted patents, as provided under 35 U.S.C. § 284;

C. A permanent injunction prohibiting Defendant from further acts of infringement of the ’630, ’612, ’323, ’708, and ’436 patents;

D. A judgment and order requiring Defendant to provide an accounting and to pay supplemental damages to Lionra, including, without limitation, pre-judgment and post-judgment interest;

E. A finding that this case is exceptional under 35 U.S.C. § 285, and an award of Lionra’s reasonable attorney’s fees and costs; and

F. Any and all other relief to which Lionra may be entitled.

Dated: August 8, 2022

/s/ Reza Mirzaie
Reza Mirzaie
CA State Bar No. 246953
Marc A. Fenster
CA State Bar No. 181067
Neil A. Rubin
CA State Bar No. 250761
RUSS AUGUST & KABAT
12424 Wilshire Boulevard, 12th Floor
Los Angeles, CA 90025
Telephone: 310-826-7474
Email: rmirzaie@raklaw.com
Email: mfenster@raklaw.com
Email: nrubin@raklaw.com

ATTORNEYS FOR PLAINTIFF,
LIONRA TECHNOLOGIES LIMITED